

Exhibit 12

Do Your Vendors Take Security Seriously?



By Tim Brown
10th September, 2020

Security



Over the past few years, security experts have increasingly emphasized the risks inherent in the software supply chain. Businesses rely on cloud applications that add complexity into an environment. The application itself could have bugs that leave an opening. Code libraries used by developers to simplify engineering could have flaws. The software could integrate with another application that may be insecure. In short, businesses do take on some additional risk in such an interconnected business environment.

That's why it's important your software vendors take their roles as business partners seriously. Their security *is* your security. When looking for a vendor selling tools for your MSP—whether it's [security tools](#), [network management](#), or [backup](#)—it's important to not only match feature lists, but also kick the tires on their security.

No software is perfect or vulnerability-free forever. But strong vendors put processes and protocols in place to reduce the risk and deal with threats if they crop up. And most importantly, strong vendors *publish* their security protocols and processes so you can evaluate whether they meet your standards. (If they don't, it's worth giving it a second thought on whether to trust them with your business and your data).

Today, we'll talk about some things to look for (and ask about) to help you make sure you can trust them with your data.

Product

When considering a vendor, start by looking at how they develop their products. Look for principles and methodologies they follow when building processes. Using strong, industry-recognized development and data privacy rules can give you assurances they take security seriously. Here are just a few to look for:

DATA PRIVACY BY DESIGN AND DEFAULT

Developments in data privacy laws around the globe increasingly require data privacy by design and default for organizations building products that handle personally identifiable information (PII). This is a major step in the right direction—rather than tacking on data privacy as an afterthought, organizations that weren't already forward-thinking on this began to emphasize data privacy more strictly. It's important to make sure organizations take steps to meet these goals by designing products with data privacy in mind *first* (by design) and making sure the strictest privacy rules apply out of the box (by default).

SECURE DEVELOPMENT LIFECYCLE

Next, try to inquire about how organizations develop their code. For example, some organizations implement the Secure Development Lifecycle (SDLC), a framework standardized by US-CERT. Following these practices increases the likelihood of producing secure products. The SDLC includes several components and practices for understanding security requirements, developing code securely, testing before code deployment, and incident response for issues that occur. (If you're curious and want to take a deep dive into the SDLC, visit [US-CERT](#).) The most important takeaway here, however, is that organizations should have a strong, mature model for developing secure products and maintaining their own security.

INFRASTRUCTURE PRACTICES

There's far more to an application's security than its code. The vendor should consistently check its own underlying infrastructure for potential issues. This means maintaining strong security controls for its systems like strong [next-generation firewalls](#), robust endpoint security for employees, password security rules and policies, vulnerability management programs, and frequent penetration testing and security posture assessments, to name a few.

PEOPLE AND PROCESSES

The underlying code is only one piece of the puzzle—vendors also need to make sure they handle the people element of their own business—from the software developer to the security professional to the non-technical finance analyst. Here are a few things to look for:

PROCESSES FOR HIRING AND OFFBOARDING

Software vendors need to make sure they have strong HR processes in place. When hiring, they should do background checks for employees, particularly in sensitive positions like systems administrators or engineers with access to sensitive data. Beyond that, they'll need to properly deal with employees during the offboarding process. While employees who lose their jobs may have an axe to grind, even employees leaving on good terms can potentially try to "help themselves" to some data on the way out. Vendors should have a series of controls and checks in place to make sure they cut off access to key data and systems when someone leaves to prevent an after-the-fact attempt to steal data, delete it, or harm the organization or its customers.

FREQUENT SECURITY AND COMPLIANCE TRAINING

The human element plays a major role in security. Despite the best efforts of security and IT teams, individual employees need to have a base level of knowledge both in terms of security and compliance. Every employee should undergo periodic security and compliance training to make sure they're on guard against potential cyberthreats.

DEDICATED SECURITY AND INCIDENT RESPONSE (IR) TEAM

Despite their best efforts, vendors will have some security incidents. They happen to *everyone*. It's just as impossible to have a perfect security posture as it is to release bug-free code. Organizations need to plan for this by having a strong incident response team and well-documented (and rehearsed) processes in the event of an actual security incident. By having an IR team in place, they can respond to incidents faster and minimize the damage (or prevent it from spreading in the first place if caught fast enough).

The bottom line

Ultimately, your vendors should have enterprise-level security and follow strict protocols and frameworks if they take your role as a partner seriously.

And to reiterate the point from the introduction, your vendors should also publish their policies and protocols. They should be transparent and give you enough information to make an informed decision before you entrust them with your business and data. Think twice before working with a company that *doesn't* publish their security policies. With the sheer number of cyberattacks, vendors have a vested interest in reassuring their customers they take their privacy and security seriously. As a result, make sure to seriously consider whether working with a vendor who doesn't publish their security policies is worth the risk.

SolarWinds MSP places a premium on the security of its products and makes sure everything is backed by sound security processes, procedures, and standards. You can learn all about the steps we take to protect your data by visiting our [Trust Center](#) today.

Tim Brown is VP of Security for SolarWinds MSP. He has over 20 years of experience developing and implementing security technology, including identity and access management, vulnerability assessment, security compliance, threat research, vulnerability management, encryption, managed security services, and cloud security. Tim's experience has made him an in-demand expert on cybersecurity, and has taken him from meeting with members of Congress and the Senate to the Situation Room in the White House. Additionally, Tim has been central in driving advancements in identity frameworks, has worked with the US government on security initiatives, and holds 18 patents on security-related topics.

Blog

1st July, 2021

Gain peace of mind and leave backup complexity behind

Backup is supposed to give you peace of mind that your customer’s data is safe. However, if you’re having to manage multiple backup solutions it can bring anything but, says...

[Read more >](#)

Blog

30th June, 2021

5 reasons why your telemarketing strategy isn’t working

Looking to get your sales pipeline running properly? Don’t be tempted to think cold calling is outdated and redundant, says Stefanie Hammond.

[Read more >](#)

Blog

29th June, 2021

The Top 7 Risks of Bring Your Own Device (BYOD) MSPs Should Remember

BYOD is on the rise—find out what this means for MSPs and read about the risks your MSP should be aware of.

[Read more >](#)

FAQ

N-able Backup: Microsoft 365 Licensing FAQ

With the growth of Microsoft 365™, it's important for businesses to make sure that data remains protected. N-able Backup offers data protection for Microsoft 365 data to help in the...

[View Resource >](#)

Video

N-able RMM: A Lightweight Desktop Management Software

[View Resource >](#)

Blog

24th June, 2021

What's new in the Automation Cookbook

In this article, we'll cover some of the most recent policies from the Automation Cookbook. Unless specified, all scripts will work with both N-central and RMM.

[Read more >](#)

Products

- N-central
- RMM
- Backup
- EDR
- Mail Assure
- Passportal
- MSP Manager
- Take Control
- Features

About us

- Leadership
- News & Press
- Careers
- Investors

Why N-able

Integrations

Contact us

Get started

English  Legal  Privacy  Cookies Settings

© 2021 N-able Solutions ULC and N-able Technologies Ltd.
All rights reserved.